Japanese Patent Laid-open No. 2003-46973 A
Publication date : Feb. 14, 2003
Applicant : Nippon Hoso Kyokai
Title : SCRAMBLING METHOD, TRANSMISSION METHOD, TRANSMISSION APPARATUS, AND RECEIVER

[0050] Furthermore, according to the present invention, an update of the scramble key used in scrambling is performed in synchronization with a coding unit of signals, or with a unit of at least one GOP (Group Of Picture). Accordingly, the scramble key in subject sections can be clearly identified, and the descrambling at the time of special reproductions can be easily performed.

[0070] Fig. 4 is one example of an embodiment of the present invention.

[0085] While the number of the Ks in the ECM is three in the explanation of the present invention, the allocated number of the Ks is not limited thereto.

[Fig. 4]
One example of embodiment of the present invention

Section I
Section II
Section III
Section IV

TS packet and its encryption key
TS packet
(Odd number 1)
(Even number 1)

(Odd number 2)

(Even number 2)

Keys in ECM transferred between each section

(Odd number 1)

(Even number 1)

(Even number 0)

(Odd number 2)

(Even number 2)

(Odd number 3)

Time

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－46973
（P2003－46973A）
(43)公開日　平成15年２月14日(2003.2.14)

(51)Int.Cl.⁷	識別記号	Ｆ Ｉ		テーマコード（参考）
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/16	Ｚ	５Ｃ０６４
7/16		7/167	Ｚ	

審査請求　未請求　請求項の数12　ＯＬ　（全 12 頁）

(21)出願番号　特願2001－232023(P2001－232023)

(22)出願日　平成13年７月31日(2001.7.31)

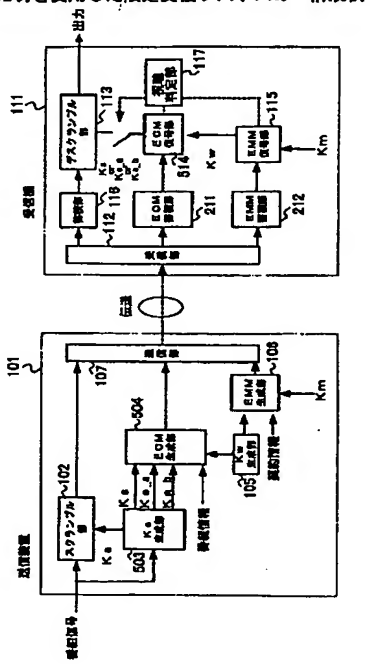
(71)出願人　000004352
日本放送協会
東京都渋谷区神南２丁目２番１号
(72)発明者　難波　誠一
東京都世田谷区砧一丁目10番11号　日本放送協会　放送技術研究所内
(72)発明者　木村　武史
東京都世田谷区砧一丁目10番11号　日本放送協会　放送技術研究所内
(74)代理人　100070150
弁理士　伊東　忠彦

Ｆターム(参考)　5C064 BA01 BB02 BC07 BC17 CA14 CB01

(54)【発明の名称】　スクランブル方法、送信方法、送信装置、及び受信機

(57)【要約】
【課題】　スクランブルされた伝送信号において、デスクランブルしながら早送り、巻き戻し等の特殊再生を可能とする信号のスクランブル方法、送信方法、送信装置、及び受信機に関する。
【解決手段】　本発明は、番組の映像や音声等の信号を区間に分割し、その区間毎に異なるスクランブル鍵Ｋｓを用いてスクランブルを行う際に、前記スクランブルを復元するための関連情報（ＥＣＭ）に含まれるＫｓの数を従来よりも増やすことにより、早送り、巻き戻し等の特殊再生時に受信者が認識可能となる映像信号及び音声信号を表示可能とする。

本発明を使用した限定受信システムの一構成例



1

【特許請求の範囲】

【請求項１】　スクランブル鍵を生成する鍵生成段階と、

前記鍵生成段階によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル段階と、

スクランブル鍵に関するスクランブル鍵情報を生成するスクランブル鍵情報生成段階とを有するスクランブル方法において、

前記スクランブル鍵情報生成段階において生成されたスクランブル鍵情報は、既に使用したスクランブル鍵に関するスクランブル鍵情報を有することを特徴とするスクランブル方法。

【請求項２】　スクランブル鍵を生成する鍵生成段階と、

前記鍵生成段階によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル段階と、

スクランブル鍵に関するスクランブル鍵情報を生成するスクランブル鍵情報生成段階とを有するスクランブル方法において、

前記スクランブル鍵情報生成段階において生成されたスクランブル鍵情報は、

現在の区間の信号のスクランブルに使用するスクランブル鍵と、

隣接する次の区間の信号のスクランブルに使用するスクランブル鍵と、

隣接する１つ前の区間の信号のスクランブルに使用するスクランブル鍵とに関する情報を少なくとも有することを特徴とするスクランブル方法。

【請求項３】　スクランブル鍵を生成する鍵生成段階と、

前記鍵生成段階によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル段階とを有するスクランブル方法において、

前記スクランブル段階は、スクランブル時に用いられるスクランブル鍵の更新を、信号の符号化単位に同期して行うことを特徴とするスクランブル方法。

【請求項４】　請求項３記載のスクランブル方法において、

前記スクランブル段階は、スクランブル時に用いられるスクランブル鍵の更新を、符号化信号の少なくとも１つのＧＯＰ単位に同期して行うことを特徴とするスクランブル方法。

【請求項５】　請求項３又は４記載のスクランブル方法により生成されたスクランブル信号と暗号化されたスクランブル鍵情報とを同時に送信する送信方法において、

前記スクランブル鍵情報は、符号化単位に同期して区切られた信号の切り替え点における直前もしくは直後、又はその両方に付加することを特徴とする送信方法。

2

【請求項６】　スクランブル鍵を生成する鍵生成部と、

前記鍵生成部によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル部と、

スクランブル鍵に関するスクランブル鍵情報を生成するスクランブル鍵情報生成部とを有する送信装置において、

前記スクランブル鍵情報生成部において生成されたスクランブル鍵情報は、既に使用したスクランブル鍵に関するスクランブル鍵情報を有することを特徴とする送信装置。

【請求項７】　スクランブル鍵を生成する鍵生成部と、

前記鍵生成部によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル部と、

スクランブル鍵に関するスクランブル鍵情報を生成するスクランブル鍵情報生成部とを有する送信装置において、

前記スクランブル鍵情報生成部において生成されたスクランブル鍵情報は、

現在の区間の信号のスクランブルに使用するスクランブル鍵と、

隣接する次の区間の信号のスクランブルに使用するスクランブル鍵と、

隣接する１つ前の区間の信号のスクランブルに使用するスクランブル鍵とに関する情報を少なくとも有することを特徴とする送信装置。

【請求項８】　スクランブル鍵を生成する鍵生成部と、

前記鍵生成部によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル部とを有する送信装置において、

前記スクランブル部は、スクランブル時に用いられるスクランブル鍵の更新を、信号の符号化単位に同期して行うことを特徴とする送信装置。

【請求項９】　請求項８記載の送信装置において、

前記スクランブル部は、スクランブル時に用いられるスクランブル鍵の更新を、符号化信号の少なくとも１つのＧＯＰ単位に同期して行うことを特徴とする送信装置。

【請求項１０】　請求項８又は９記載の送信装置により生成されたスクランブル信号と暗号化されたスクランブル鍵情報とを同時に送信する送信装置において、

前記スクランブル鍵情報は、符号化単位に同期して区切られた信号の切り替え点における直前もしくは直後、又はその両方に付加することを特徴とする送信装置。

【請求項１１】　スクランブル鍵によりスクランブルされた信号を受信する受信部と、

スクランブル信号を蓄積する蓄積部と、

スクランブル鍵情報を復号するスクランブル鍵情報復号部と、

スクランブル信号をデスクランブルするデスクランブル

3

部とを有する受信機において、
前記スクランブル鍵情報復号部において復号されたデスクランブル鍵情報は、既に使用したデスクランブル鍵に関するデスクランブル鍵情報を有することを特徴とする受信機。
【請求項１２】　スクランブル鍵によりスクランブルされた信号を受信する受信部と、
スクランブル信号を蓄積する蓄積部と、
スクランブル鍵情報を復号するスクランブル鍵情報復号部と、
スクランブル信号をデスクランブルするデスクランブル部とを有する受信機において、
前記スクランブル鍵情報復号部において復号されたデスクランブル鍵情報は、
現在の区間の信号のデスクランブルに使用するデスクランブル鍵と、
隣接する次の区間の信号のデスクランブルに使用するデスクランブル鍵と、
隣接する１つ前の区間の信号のデスクランブルに使用するデスクランブル鍵とに関する情報を少なくとも有することを特徴とする受信機。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】スクランブル方法、送信方法、送信装置、及び受信機に関する。
【０００２】
【従来の技術】放送サービスを伝送する電波は誰でも受信することができる。このため、電波が受信できても番組やサービスの内容が判別できないように情報を秘匿する処理を行っている。これは一般にスクランブルと呼ばれている。
【０００３】ところで、記録された信号を再生し視聴する場合において、特に早送りや巻き戻しを行う、いわゆる特殊再生機能を要する場合、従来技術ではスクランブルが行われていない状態（受信側においては、デスクランブルされた状態）で記録するため、アナログ信号と同様に、ある程度までの速度範囲であれば、内容が理解できるような画質の再生を可能にしていた。
【０００４】しかし、例えば、ペイパービュー（以下ＰＰＶ とする）方式による番組のような場合、デスクランブルを行う時に課金処理が行われるため、一時的に種々の番組を記録しておき、希望する時間にそれらから選択して番組を視聴するといういわゆるホームサーバーとして利用するような状況では、最終的には見ない番組にも課金されてしまうという問題がある。
【０００５】ここで、前記の内容を図を用いて説明する。
【０００６】図１は、従来の限定受信システムの第一の構成例である。
【０００７】図１において、従来の限定受信システムは

4

送信装置１０１、及び受信機１１１より構成されている。
【０００８】送信装置１０１は、スクランブル部１０２、Ｋｓ（スクランブル鍵）生成部１０３、ＥＣＭ生成部１０４、Ｋｗ（ワーク鍵）生成部１０５、ＥＭＭ生成部１０６、送信部１０７より構成されている。
【０００９】また、受信機１１１は、受信部１１２、デスクランブル部１１３、ＥＣＭ復号部１１４、ＥＭＭ復号部１１５、蓄積部１１６、視聴判定部１１７より構成されている。
【００１０】送信装置１０１に番組信号が入力されると、スクランブル部１０２はＫｓを用いて番組信号をスクランブルする。Ｋｓ生成部１０３は、スクランブル部１０２及びＥＣＭ生成部１０４に同一のＫｓを出力する。ＥＣＭ生成部１０４は、Ｋｓ及び番組の種類や時刻、視聴料金等の属性情報（以下 番組情報 とする）をＫｗを用いて暗号化し、ＥＣＭ（Entitlement Control Message）を生成する。Ｋｗ生成部１０５は、ＥＣＭ生成部１０４及びＥＭＭ生成部１０６に同一のＫｗを出力する。ＥＭＭ生成部１０６は、Ｋｗ及び受信者の契約したチャンネル、又は契約有効期限等の契約内容の情報（以下 契約情報 とする）を、Ｋｍ（マスタ鍵）を用いて暗号化を行い、ＥＭＭ（Entitlement Management Message）を生成する。送信部１０７は、スクランブル信号、ＥＣＭ、ＥＭＭを送信する。
【００１１】受信機１１１は伝送されたスクランブル信号を受信部１１２が受け取り、スクランブル信号はデスクランブル部１１３へ、ＥＣＭ信号はＥＣＭ復号部１１４へ、ＥＭＭ信号はＥＭＭ復号部１１５へ出力される。
【００１２】ＥＭＭ復号部１１５は予め与えられているＫｍを用いてＥＭＭの復号を行う。ＥＣＭ復号部１１４はＥＭＭ復号部１１５で取得されたＫｗを用いて復号を行う。視聴判定部１１７は、ＥＭＭ復号部１１５にて復号された契約情報とＥＣＭ復号部１１４にて復号された番組信号とを用いて、受信したスクランブル信号が受信者との契約上視聴可能な信号であるかを判定し、視聴可能であった場合、取得されたＫｓをデスクランブル部１１３に与えてデスクランブルを行う。これらＥＣＭ復号部１１４、ＥＭＭ復号部１１５、及び視聴判定部１１７は、ＣＰＵ（Central Processing Unit）内蔵のＩＣ（Integrated Circuit）カードの中の処理プログラムとして実現されることも多い。デスクランブルされた信号は蓄積部１１６に蓄積され、特殊再生を含む再生が行われる。
【００１３】番組信号が送信装置１０１に入力されると、スクランブル部１０２はＫｓ生成部１０３から入力されたＫｓを用いてスクランブルを行い、送信部１０７へ出力する。Ｋｓは番組情報と共にＥＣＭ生成部１０４へ入力する。ＥＣＭ生成部１０４は、Ｋｓと番組情報とからＥＣＭを生成し、Ｋｗ生成部１０５より入力された

5

Ｋｗを用いて暗号化した後、送信部１０７へ出力する。なお、Ｋｓは従来技術においては、時間単位（１秒程度）で更新されている。また、ＫｗはＥＣＭの暗号を解読するために必要な鍵であり、１ヶ月～１年程度で更新を行うよう想定されている。Ｋｗは契約情報と共にＥＭＭ生成部１０６に入力し、Ｋｗと契約情報とからＥＭＭを生成し、Ｋｍを用いて暗号化した後、送信部１０７へ出力する。送信部１０７は、スクランブル信号、ＥＣＭ、ＥＭＭを送信する。

【００１４】受信機１１１では、伝送信号を受信部１１２で受信し、スクランブル信号をデスクランブル部１１３へ、ＥＣＭをＥＣＭ復号部１１４へ、ＥＭＭをＥＭＭ復号部１１５へ出力する。その後、ＥＭＭ復号部１１５でＫｍを用いてＥＭＭの復号を行い、契約情報及びＫｗを取得する。ＥＣＭ復号部１１４はＥＭＭ復号部１１５から入力されたＫｗ用いて復号を行い、Ｋｓ及び番組情報を取得する。

【００１５】ここで、先ほどＥＭＭ復号部１１５にて復号された契約情報とＥＣＭ復号部１１４にて復号された番組信号とから、受信信号が受信者にとって視聴可能な信号であるかを視聴判定部１１７で判定し、視聴可能な信号であった場合、デスクランブル部１１３にＫｓを送り、スクランブル信号のデスクランブルを行う。デスクランブルされた信号は、蓄積部１１６で蓄積され、受信者の希望する出力方法で出力する。従来のシステムでは、デスクランブルされた信号が蓄積されているため、早送り、巻き戻し等の特殊再生も可能となる。

【００１６】しかしながら、ＰＰＶ方式による番組のような場合、デスクランブルを行う時に課金処理が行われるため、蓄積部１１６に蓄積した信号は、受信者が視聴しない場合においても、既に課金されていることになる。

【００１７】そこで次に、受信者が視聴した番組だけが課金されるようにした従来の限定受信システムの第二の構成例を図２に示す。

【００１８】図２において、従来の限定受信システムは送信装置１０１、及び受信機１１１より構成されている。送信装置１０１は、スクランブル部１０２、Ｋｓ生成部１０３、ＥＣＭ生成部１０４、Ｋｗ生成部１０５、ＥＭＭ生成部１０６、送信部１０７より構成されている。また、受信機１１１は、受信部１１２、デスクランブル部１１３、ＥＣＭ復号部１１４、ＥＭＭ復号部１１５、蓄積部１１６、視聴判定部１１７、ＥＣＭ蓄積部２１１、ＥＭＭ蓄積部２１２より構成されている。

【００１９】図２の限定受信システムにおける送信装置１０１の動作内容は、図１の送信装置１０１と同様であるため、説明を省略する。

【００２０】受信機１１１において、伝送信号を受信部１１２で受信し、スクランブル信号を蓄積部１１６へ、ＥＣＭをＥＣＭ蓄積部２１１へ、ＥＭＭをＥＭＭ蓄積部

6

２１２へ出力する。蓄積部１１６にはスクランブルされたままの信号が蓄積される。ＥＭＭ蓄積部２１２は、ＥＭＭ信号を復号せずにそのまま蓄積する。ＥＭＭ復号部１１５はＫｍを用いてＥＭＭの復号を行う。ＥＣＭ復号部１１４はＥＭＭ復号部１１５で取得されたＫｗを用いて復号を行う。ここで、先ほどＥＭＭ復号部１１５にて復号された契約情報とＥＣＭ復号部１１４にて復号された番組信号とから、受信信号が受信者にとって視聴可能な信号であるかを視聴判定部１１７で判定し、視聴可能な信号であった場合、取得されたＫｓを用いてデスクランブル部１１３にてデスクランブルを行い出力する。これらＥＣＭ復号部１１４、ＥＭＭ復号部１１５、及び視聴判定部１１７は、ＣＰＵ内蔵のＩＣカードの中の処理プログラムとして実現されることも多い。

【００２１】送信装置１０１から伝送された信号は、受信部１１２で受信する。その後、スクランブル信号は蓄積部１１６にスクランブルされた信号のまま蓄積される。同様にＥＣＭはＥＣＭ蓄積部２１１に、ＥＭＭはＥＭＭ蓄積部２１２に夫々蓄積される。

【００２２】ここで、受信者が蓄積部１１６にある特定の番組情報を視聴する指示をした場合、受信機１１１は、まずＥＭＭ復号部１１５が、ＥＭＭ蓄積部２１２に蓄積されている指定された番組信号に対応したＥＭＭを復号し、Ｋｗ及び契約情報を取得する。ＥＣＭ復号部１１４はＥＣＭ蓄積部２１１より受信者が指定した番組情報に対応したＥＣＭを復号し、Ｋｓ及び番組情報を取得する。ＥＭＭ復号部１１５にて取得した契約情報とＥＣＭ復号部１１４にて取得した番組情報とから受信者が視聴可能な番組か否かの判定を行い、視聴可能であった場合、デスクランブル部１１３にＫｓを出力する。デスクランブル出力部１１３は蓄積部より、受信者が指示した番組のスクランブル信号をＫｓを用いてデスクランブルし、出力する。

【００２３】しかしながら、図２の受信システムの場合、蓄積を対象としない放送信号を蓄積した後、再生して視聴しているので、受信機１１１においてＥＣＭ復号部１１４より送られるＫｓでは、放送された信号と同じ順序で再生されるスクランブル信号のデスクランブルは行えるが、逆の順序で再生されるスクランブル信号がデスクランブル部１１３に入力される前にその対応するＫｓを取得することができない。

【００２４】

【発明が解決しようとする課題】上記のように、従来の限定受信システムでは、特殊再生処理を行うために事前にデスクランブルした信号を蓄積するシステム構成の場合、実際には視聴していない番組でも課金されてしまうという問題があった。又、視聴した番組のみ課金対象となるようなシステム構成の場合、特殊再生処理ができないという問題があった。

【００２５】本発明は、上記問題点に鑑みなされたもの

であり、スクランブル方法、送信方法、送信装置、及び受信機を提供することを目的とする。

【００２６】

【課題を解決するための手段】上記課題を解決するために、本件発明は、以下の特徴を有する課題を解決するための手段を採用している。

【００２７】請求項１に記載された発明は、スクランブル鍵を生成する鍵生成段階と、前記鍵生成段階によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル段階と、スクランブル鍵に関するスクランブル鍵情報を生成するスクランブル鍵情報生成段階とを有するスクランブル方法において、前記スクランブル鍵情報生成段階において生成されたスクランブル鍵情報は、既に使用したスクランブル鍵に関するスクランブル鍵情報を有することを特徴とする。

【００２８】請求項１記載の発明によれば、スクランブル信号をデスクランブルする際に、特に巻き戻し再生に必要となるスクランブル鍵を容易に取得することができる。

【００２９】請求項２に記載された発明は、スクランブル鍵を生成する鍵生成段階と、前記鍵生成段階によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル段階と、スクランブル鍵に関するスクランブル鍵情報を生成するスクランブル鍵情報生成段階とを有するスクランブル方法において、前記スクランブル鍵情報生成段階において生成されたスクランブル鍵情報は、現在の区間の信号のスクランブルに使用するスクランブル鍵と、隣接する次の区間の信号のスクランブルに使用するスクランブル鍵と、隣接する１つ前の区間の信号のスクランブルに使用するスクランブル鍵とに関する情報を少なくとも有することを特徴とする。

【００３０】請求項２記載の発明によれば、スクランブル信号をデスクランブルする際に早送り、巻き戻し等の特殊再生を容易に行うことができる。

【００３１】請求項３に記載された発明は、スクランブル鍵を生成する鍵生成段階と、前記鍵生成段階によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル段階とを有するスクランブル方法において、前記スクランブル段階は、スクランブル時に用いられるスクランブル鍵の更新を、信号の符号化単位に同期して行うことを特徴とする。

【００３２】請求項３記載の発明によれば、例えば、早送り、巻き戻し等の特殊再生を行う場合に、符号化単位、又はその整数倍の区切りでスクランブル鍵の更新を行うことで、その区間のスクランブル鍵を明確にし、特殊再生時のデスクランブル時に容易に画像もしくは音声を表示させることができる。

【００３３】請求項４に記載された発明は、請求項３記載のスクランブル方法において、前記スクランブル段階

は、スクランブル時に用いられるスクランブル鍵の更新を、符号化信号の少なくとも１つのＧＯＰ単位に同期して行うことを特徴とする。

【００３４】請求項４記載の発明によれば、スクランブル信号のある区間におけるスクランブル鍵を明確にし、特殊再生時のデスクランブル時に容易に画像もしくは音声を表示させることができる。

【００３５】請求項５に記載された発明は、請求項３又は４記載のスクランブル方法により生成されたスクランブル信号と暗号化されたスクランブル鍵情報とを同時に送信する送信方法において、前記スクランブル鍵情報は、符号化単位に同期して区切られた信号の切り替え点における直前もしくは直後、又はその両方に付加することを特徴とする。

【００３６】請求項５記載の発明によれば、スクランブル信号をデスクランブルする際に早送り、巻き戻し等の特殊再生時にも受信者が待ち時間なく、映像信号、又は音声信号の再生を容易に行うことができる。

【００３７】請求項６に記載された発明は、スクランブル鍵を生成する鍵生成部と、前記鍵生成部によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル部と、スクランブル鍵に関するスクランブル鍵情報を生成するスクランブル鍵情報生成部とを有する送信装置において、前記スクランブル鍵情報生成部において生成されたスクランブル鍵情報は、既に使用したスクランブル鍵に関するスクランブル鍵情報を有することを特徴とする。

【００３８】請求項７に記載された発明は、スクランブル鍵を生成する鍵生成部と、前記鍵生成部によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル部と、スクランブル鍵に関するスクランブル鍵情報を生成するスクランブル鍵情報生成部とを有する送信装置において、前記スクランブル鍵情報生成部において生成されたスクランブル鍵情報は、現在の区間の信号のスクランブルに使用するスクランブル鍵と、隣接する次の区間の信号のスクランブルに使用するスクランブル鍵と、隣接する１つ前の区間の信号のスクランブルに使用するスクランブル鍵とに関する情報を少なくとも有することを特徴とする。

【００３９】請求項８に記載された発明は、スクランブル鍵を生成する鍵生成部と、前記鍵生成部によって生成されたスクランブル鍵により、符号化された信号をスクランブルするスクランブル部とを有する送信装置において、前記スクランブル部は、スクランブル時に用いられるスクランブル鍵の更新を、信号の符号化単位に同期して行うことを特徴とする。

【００４０】請求項９に記載された発明は、請求項８記載の送信装置において、前記スクランブル部は、スクランブル時に用いられるスクランブル鍵の更新を、符号化信号の少なくとも１つのＧＯＰ単位に同期して行うこと

9

を特徴とする。

【００４１】請求項１０に記載された発明は、請求項８又は９記載の送信装置により生成されたスクランブル信号と暗号化されたスクランブル鍵情報とを同時に送信する送信装置において、前記スクランブル鍵情報は、符号化単位に同期して区切られた信号の切り替え点における直前もしくは直後、又はその両方に付加することを特徴とする。

【００４２】請求項６から１０に記載された発明によれば、請求項１乃至４何れか一項記載のスクランブル方法、又は請求項５の送信方法に適した送信装置を提供することができる。

【００４３】請求項１１に記載された発明は、スクランブル鍵によりスクランブルされた信号を受信する受信部と、スクランブル信号を蓄積する蓄積部と、スクランブル鍵情報を復号するスクランブル鍵情報復号部と、スクランブル信号をデスクランブルするデスクランブル部とを有する受信機において、前記スクランブル鍵情報復号部において復号されたデスクランブル鍵情報は、既に使用したデスクランブル鍵に関するデスクランブル鍵情報を有することを特徴とする。

【００４４】請求項１１の発明によれば、逆方向（巻き戻し）再生を行いながら、デスクランブルを行うことができる受信機を提供することができる。

【００４５】請求項１２に記載された発明は、スクランブル鍵によりスクランブルされた信号を受信する受信部と、スクランブル信号を蓄積する蓄積部と、スクランブル鍵情報を復号するスクランブル鍵情報復号部と、スクランブル信号をデスクランブルするデスクランブル部とを有する受信機において、前記スクランブル鍵情報復号部において復号されたデスクランブル鍵情報は、現在の区間の信号のデスクランブルに使用するデスクランブル鍵と、隣接する次の区間の信号のデスクランブルに使用するデスクランブル鍵と、隣接する１つ前の区間の信号のデスクランブルに使用するデスクランブル鍵とに関する情報を少なくとも有することを特徴とする。

【００４６】請求項１２の発明によれば、早送り、巻き戻し等の特殊再生を行いながら、デスクランブルを行うことができる受信機を提供することができる。

【００４７】

【発明の実施の形態】本発明は、特殊再生処理を行いながらデスクランブル行うことができる信号のスクランブル方法、送信方法、送信装置、及び受信機を提供することを主眼とする。

【００４８】本発明は、スクランブルがかかった信号のままで記録した信号に早送り、巻き戻し等の特殊再生を行う場合に、デスクランブル時に鍵の再生が間に合わないことがないよう、現在の区間に対応するスクランブル鍵Ｋｓの他に、隣接する一つ先の区間の信号のスクランブルに使用するスクランブル鍵Ｋｓ_ａ、隣接する一つ

10

前の区間の信号のスクランブルに使用するスクランブル鍵Ｋｓ_ｂをもスクランブルを復元するための関連情報（ＥＣＭ）に記録することにより、特殊再生時にも受信者が待ち時間なく、映像信号、又は音声信号を表示できるようにする。

【００４９】なお、（社）電波産業会（ＡＲＩＢ）の標準規格「ＢＳデジタル放送限定受信方式」（ＡＲＩＢ ＳＴＤ－Ｂ２５）によれば、ＥＣＭセクション構造にはスクランブル鍵（Ｏｄｄ）、スクランブル鍵（Ｅｖｅｎ）があり、「現在と次の、２つのスクランブル鍵をペアで送る。」との記載があるが、一つ前のスクランブル鍵とペアで送る規格及び現在と次と一つ前の３個のスクランブル鍵が存在するＥＣＭセクション構造の規格はまだない。

【００５０】また、本発明はスクランブル時に用いられるスクランブル鍵の更新を、信号の符号化単位、又は少なくとも１つのＧＯＰ（Group Of Picture）単位に同期して行うことにより、その区間のスクランブル鍵を明確にし、特殊再生時のデスクランブルを容易に行うことができる。

【００５１】なお、スクランブル鍵情報においては、Ｋｓ_ａ及びＫｓ_ｂは、符号化単位に同期して区切られた信号の切り替え点の直前もしくは直後、又はその両方に付加することにより、次の区間までの時間が短い場合、又は高速な特殊再生を行う場合等において、次にデスクランブルされる区間に対応する鍵をより確実に再生することができる。

【００５２】デジタル放送における限定受信方式は、例えば、ＡＲＩＢの標準規格ＡＲＩＢＳＴＤ－Ｂ２５に示されているように、映像信号や音声信号はデジタル符号化され、ＭＰＥＧ多重化方式の規格で示されるようなＴＳパケットのペイロード部分に載せて送られる。

【００５３】信号をスクランブルして伝送する場合には、ＴＳパケットのペイロード部分がブロック暗号方式で暗号化される。この暗号化と復号に使用されるスクランブル鍵Ｋｓは、番組情報と共に、ＥＣＭとして構成され、スクランブルされた信号と同じ伝送路で受信機に送られる。

【００５４】このＥＣＭは秘密の鍵情報を含むことから、ワーク鍵Ｋｗと呼ばれる鍵で暗号化して送られる。

【００５５】受信機では、まずこのＥＣＭの暗号を復号してＫｓを取得し、これを用いて信号のスクランブルを復元する。このとき、ＥＣＭの暗号化データの復号には時間が必要であり、この復号時間を経た後でなければ、デスクランブルすることができない。復号時間は受信機回路の性能によっても変わるので、Ｋｓを一つしか送らないシステムでは、全ての受信機で暗号化データの復号が完了した後でなければ、そのＫｓを用いて信号をデスクランブルすることはできず、この時間が、チャンネルを切り替えたときに番組が受信されるまでの待ち時間と

なっていた。

【００５６】このため、ＢＳデジタル放送の限定受信システム（ＣＡＳ（Conditional Access System））では、一つのＥＣＭの中に奇数期間と偶数期間に使用するＫｓを別個に設けている。

【００５７】信号の各ＴＳパケットがいずれのＫｓでスクランブルされているかは、各ＴＳパケットのヘッダ内に存在するスクランブル制御フラグの値によって識別される。

【００５８】ここで、これら二つのＫｓによる信号のスクランブル（ＴＳパケットのヘッダのスクランブル制御フラグの値）とＥＣＭで送るＫｓの時間の関係を示すと図３のようになる。

【００５９】図３は、時間の経過と共に各区間で、ある特定のＫｓによりスクランブルされたＴＳパケットと各区間で送られるＥＣＭ信号との関連を示した従来のスクランブル信号とＥＣＭの関連図である。

【００６０】図３において、例えば区間IIに含まれるＴＳパケット２はＫｓ（偶1）でスクランブルが行われ、区間IIIに含まれるＴＳパケット３はＫｓ（奇２）でスクランブルが行われている。なお、時間はＴ１からＴ２へと経過していくものとする。

【００６１】この信号において、デスクランブルを行うためのＥＣＭを送るＴＳパケットは、ＭＰＥＧ多重方式ではスクランブルした信号を送るＴＳパケットの間に時分割で多重化されて送られるが、区間IIの信号をデスクランブルするためのＥＣＭは一般的には、区間Iの開始直後すなわち時刻Ｔ１の直後に送られる。

【００６２】受信機ではこのＥＣＭを受信して暗号化データの復号を行うと、Ｋｓ（偶1）とＫｓ（奇1）が得られる。

【００６３】従って、Ｔ１の直後に受信したＥＣＭを復号処理する時間が時間（Ｔ２－Ｔ１）の間隔より長くならなければ、区間IIの信号が受信される前に、Ｋｓ（偶1）が得られ、正しくデスクランブルできることになる。

【００６４】このような方法をとることにより、ＥＣＭの復号処理が終了すると同時にＫｓによるデスクランブルが可能となる。

【００６５】一方、放送の場合は番組の途中から受信することが多いので、受信を開始して最初に受信されたＥＣＭを復号したとき、Ｋｓ（奇1）が得られれば、区間Iの途中からでもデスクランブルが可能になり、Ｔ２まで待つ必要がなくなる。

【００６６】この途中受信の場合の待ち時間を少なくするために、各区間の途中でも図３に示したように、その区間内でのＫｓとその先のＫｓ（Ｋｓ_ａ）を含むＥＣＭが伝送されるのが一般的である。

【００６７】ところで、図３に示したＴ１→Ｔ２→Ｔ３→Ｔ４といった時間順序で番組の信号が記録された場

合、今スクランブルが行われていない視聴可能な番組信号を考えると、後に述べるように、受信機に適当な蓄積部を用意することにより、Ｔ４→Ｔ３→Ｔ２→Ｔ１といった逆方向に再生する場合に映像等を再生することが可能となる。

【００６８】しかし、スクランブルが行われている信号に対し、Ｔ４→Ｔ３→Ｔ２→Ｔ１といった逆方向に再生する場合には、図３の構成では、スクランブル信号に対応するＥＣＭを取得して暗号化データを復号しても、得られるＫｓは逆方向に進行する区間のものであり、その次の区間のＫｓ（Ｋｓ_ｂ）を取得することができず、連続的に信号をデスクランブルすることはできない。

【００６９】そこで、逆方向への再生が可能となるような本発明の実施の形態を図４に示す。

【００７０】図４は、本発明実施の一例の図である。

【００７１】図４は図３と同様に、時間の経過と共に各区間である特定のＫｓによりスクランブルされた少なくとも１つのＧＯＰ（Group Of Picture）単位で生成されたＴＳパケットと、各区間で送られるＥＣＭ信号との関連を示したものである。

【００７２】図４において、順方向と逆方向（巻き戻し）のいずれの再生の場合にも利用できるようなＫｓを配置したＥＣＭを生成する。

【００７３】例えば、区間IIで再生されたＥＣＭの暗号を復号すると、その区間に使用されているＫｓ（偶１）と共に、Ｋｓ（奇２）とＫｓ（奇１）が得られる。

【００７４】ここで、図４の各区間で送られるＥＣＭ内の鍵において、上部に記載されているＫｓを現区間のＴＳパケットを再生する場合のＫｓとし、中部に記載のＫｓを順方向再生の場合に使用するＫｓとし、下部に記載のＫｓを逆方向再生の場合に使用するＫｓとする。

【００７５】例えば、区間IIで再生されたＥＣＭの暗号を復号すると、その区間に使用されているＫｓ（偶１）と共に、Ｋｓ（奇２）とＫｓ（奇１）が得られる。

【００７６】Ｋｓ（奇２）は順方向再生の場合に使用し、Ｋｓ（奇１）は逆方向再生の場合に使用する。従って、区間IIの後に区間Iの信号が再生されても、Ｋｓ（奇１）を用いて正しくデスクランブルすることができる。

【００７７】なお、順方向の早送りや巻き戻しで高速に再生する場合には、区間の時間長とＥＣＭの暗号、復号に要する時間の比に対応する速度比までが正しくデスクランブルできる範囲となる。

【００７８】次に、特殊再生と信号のＴＳパケットの関係について述べる。ここで、信号として映像信号を考えると、デジタル放送等で多く使用されているＭＰＥＧ－２の画像符号化方式ではフレーム内符号化、フレーム間予測符号化が組み合わされており、フレーム内符号化を行うフレームをＩピクチャという。また、フレーム間予測符号化では、順方向予測による符号化を行うフレーム

13

をＰピクチャといい、両方向予測による符号化を行うフレームをＢピクチャという。前記のピクチャタイプにより画像フレームが組み合わされている。これらはＧＯＰ（Group Of Picture）と呼ばれる単位（例えば０．５秒間の映像に対応）で処理されるのが一般的である。

【００７９】いま、記録された映像信号を逆方向で再生して、受信者が認識可能な画像を再現する場合には、例えば、ＧＯＰ単位又はその整数倍の画像に対応する分のＴＳパケットをまとめてバッファメモリ等に記録して、逆方向再生等の処理を行うのが適当である。

【００８０】この点から、映像信号をスクランブルする場合のＫｓは、この画像符号化の単位に関連した区間で更新することが適当であるといえる。

【００８１】また、本発明は、スクランブルを行うＫｓの奇数、偶数を切り替える時点を、画像符号化の適当な単位の境界とする方法と装置を与えるものである。この切替えの単位としては、例えば、前述のＧＯＰ単位あるいは複数のＧＯＰ単位とするのが適当である。

【００８２】記録された信号を早送り等の高速で再生する場合に映像等を出力するには、バッファメモリ等に記録した後、処理を行って出力するが、高速で再生されるので、一部の映像信号と音声信号を抽出して提示することになる。

【００８３】このとき、信号にスクランブルが行われている場合には、デスクランブルを行った上で処理する必要がある。

【００８４】なお、ＭＰＥＧ－２の画像符号化方式と多重化方式では、符号化された各ピクチヤはＰＥＳ（Packetized Elementary Stream）パケットと呼ばれるパケットに構成され、これを分割してＴＳパケットのペイロード部分に入れて伝送、あるいは記録されるが、ＭＰＥＧの規格では一つのＴＳパケットに複数のＰＥＳパケットの信号が入ることはないので、ＴＳパケットのスクランブル鍵Ｋｓを確実に区別することができる。

【００８５】なお、本発明の説明で、各区間で送られるＥＣＭ内のＫｓの数を３つとしたが、付与できる数は、この限りではない。

【００８６】ここで、本発明を使用した実施例を図面を用いて説明する。

【００８７】図５は、本発明を使用した限定受信システムの一構成例である。

【００８８】図５において、本発明を使用した限定受信システムは送信装置１０１、受信機１１１より構成されている。送信装置１０１は、スクランブル部１０２、Ｋｓ生成部５０３、ＥＣＭ生成部５０４、Ｋｗ生成部１０５、ＥＭＭ生成部１０６、送信部１０７より構成されている。また、受信機１１１は、受信部１１２、デスクランブル部１１３、ＥＣＭ復号部５１４、ＥＭＭ復号部１１５、蓄積部１１６、視聴判定部１１７、ＥＣＭ蓄積部２１１、ＥＭＭ蓄積部２１２より構成されている。

14

【００８９】送信装置１０１に番組信号が入力されると、スクランブル部１０２とＫｓ生成部５０３に入力される。Ｋｓ生成部５０３はＴＳパケットに対してＫｓを生成し、スクランブル部１０２に出力する。スクランブル部１０２は、番組信号をＫｓを用いてスクランブルを行う。

【００９０】Ｋｓ生成部５０３は、ＥＣＭ生成部５０４に対し、現在のＴＳパケット信号に対するスクランブル鍵Ｋｓの他に、時間的に未来に位置する隣接したＴＳパケット信号のスクランブル鍵Ｋｓ_ａと時間的に過去に位置する隣接したＴＳパケット信号のスクランブル鍵Ｋｓ_ｂとを出力する。ＥＣＭ生成部５０４は、Ｋｓ、Ｋｓ_ａ、Ｋｓ_ｂと番組情報をＫｗ生成部１０５から入力されるＫｗを用いて暗号化しＥＣＭを生成する。Ｋｗ生成部１０５は、ＥＣＭ生成部に出力したＫｗと同一のＫｗをＥＭＭ生成部１０６に出力する。ＥＭＭ生成装置１０６では、Ｋｗと契約情報からＫｍを用いて暗号化しＥＭＭを生成する。送信部１０７は、スクランブル信号、ＥＣＭ、ＥＭＭを送信する。

【００９１】送信装置１０１から伝送されたスクランブル信号、ＥＣＭ、ＥＭＭは受信部１１２で受信されると、スクランブル信号は蓄積部１１６にスクランブル信号のまま蓄積される。ＥＣＭはＥＣＭ蓄積部２１１に、ＥＭＭはＥＭＭ蓄積部２１２に蓄積される。その後、ＥＭＭ復号部１１５でマスタ鍵を用いてＥＭＭ信号を復号し、Ｋｗ及び契約情報を取得する。ＥＣＭ復号部５１４では、復号したＫｗを用いてＥＣＭ信号の復号を行い、Ｋｓ、Ｋｓ_ａ、Ｋｓ_ｂ、及び番組情報を取得する。

【００９２】次に、蓄積部１１６に蓄積しているスクランブルされた番組の再生方法を選択する。再生方法には、通常再生の他に、早送り再生、巻き戻し再生等の特殊再生が存在する。視聴判定部１１７は、ＥＭＭ復号部１１５で復号された契約情報、及びＥＣＭ復号部５１４で復号された番組情報から、選択されたスクランブル信号が受信者との契約上視聴可能であるかを判定し、視聴可能であった場合、選択された再生方法に従い、その対応したスクランブル鍵をデスクランブル部１１３に送る。デスクランブル部１１３は、指示された再生方法に従ってデスクランブルを行い出力する。

【００９３】前記から送信装置１０１、及び受信機１１１を使用することにより、受信者が視聴を希望した番組のみにデスクランブルを行うことができ、さらに、早送り、巻き戻し等の特殊再生を行うことができる。

【００９４】本発明を利用することにより、例えば、ＣＡＴＶ等のケーブル伝送路を介して、放送局側のビデオサーバーから希望の映画等の番組にスクランブルをかけて配信する場合に、受信側からの操作で画面を確認しながら巻き戻すといった特殊再生を行うことができるようになる。このシステム構成が、単純にサーバーにはスクランブルされていない信号を蓄積し、再生した後でスク

15

ランブルを行って伝送する場合には、従来の技術において実現できるが、その場合、受信する人の数だけスクランブラが必要になり、放送のような多数の受信者を対象とするシステムでは現実的ではない。

【００９５】従って、スクランブルされた信号をサーバーに記録しておき、この再生の制御のみを受信者ごとに行えるようにするシステムが好適であるといえる。

【００９６】本発明を実施することにより、スクランブルされて伝送された信号を特殊再生しながら、デスクランブルして視聴することができる。

【００９７】

【発明の効果】本発明は、特殊再生処理を行いながら、デスクランブルを行うことができる信号のスクランブル方法、送信方法、送信装置、及び受信機を提供することができる。

【図面の簡単な説明】

【図１】従来の限定受信システムの第一の構成例である。

【図２】従来の限定受信システムの第二の構成例である。

【図３】従来のスクランブル信号とＥＣＭの関連図である。

16

る。

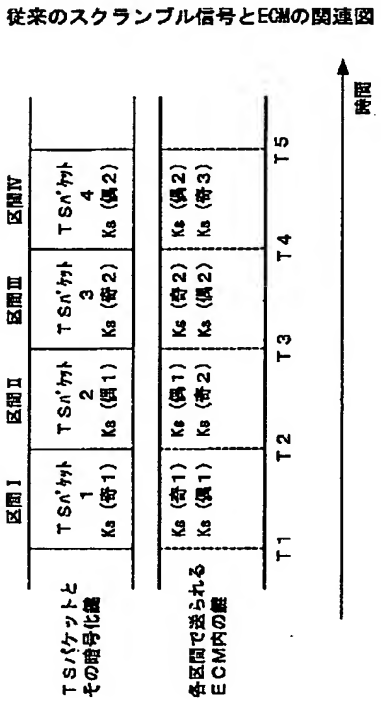
【図４】本発明実施の一例の図である。

【図５】本発明を使用した限定受信システムの一構成例である。

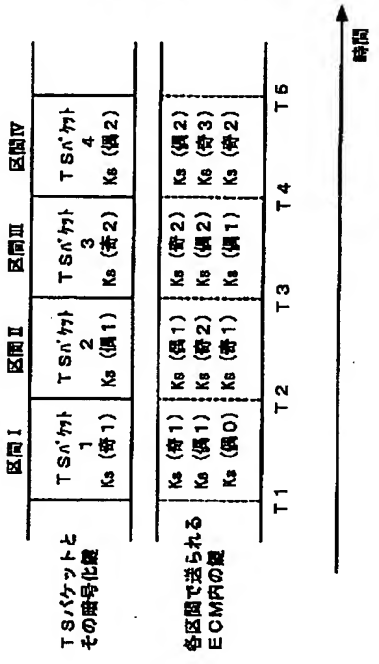
【符号の説明】

１０１　送信装置
１０２　スクランブル部
１０３、５０３　Ｋｓ生成部
１０４、５０４　ＥＣＭ生成部
１０５　Ｋｗ生成部
１０６　ＥＭＭ生成部
１０７　送信部
１１１　受信機
１１２　受信部
１１３　デスクランブル部
１１４、５１４　ＥＣＭ復号部
１１５　ＥＭＭ復号部
１１６　蓄積部
１１７　視聴判定部
２１１　ＥＣＭ蓄積部
２１２　ＥＭＭ蓄積部

【図３】

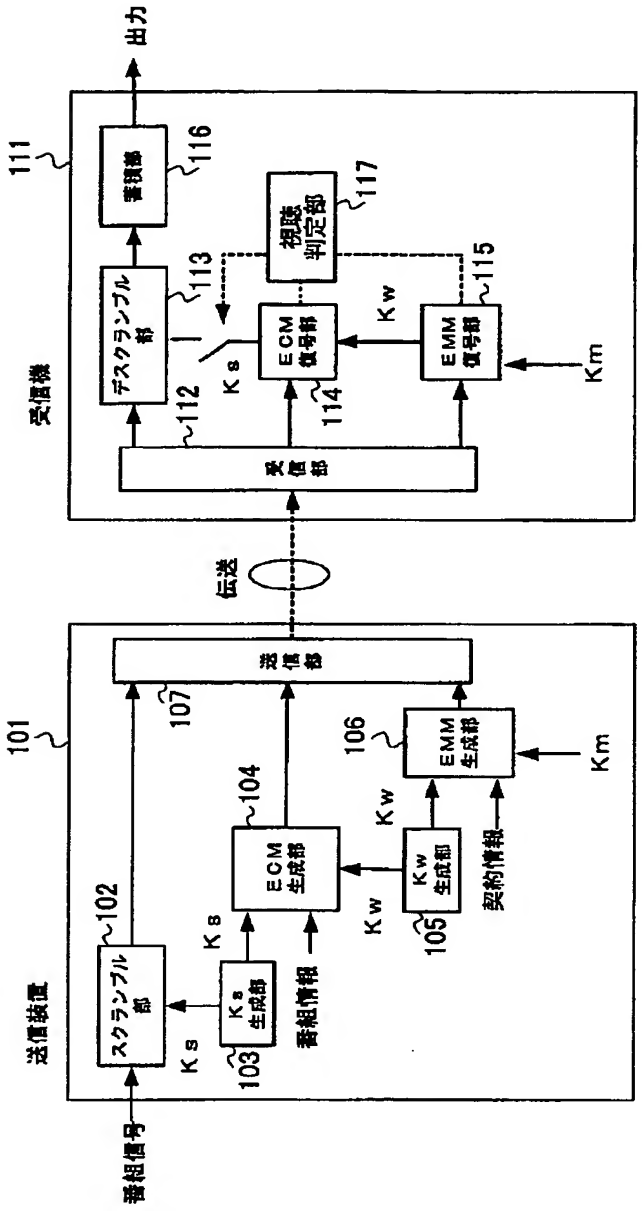


【図４】



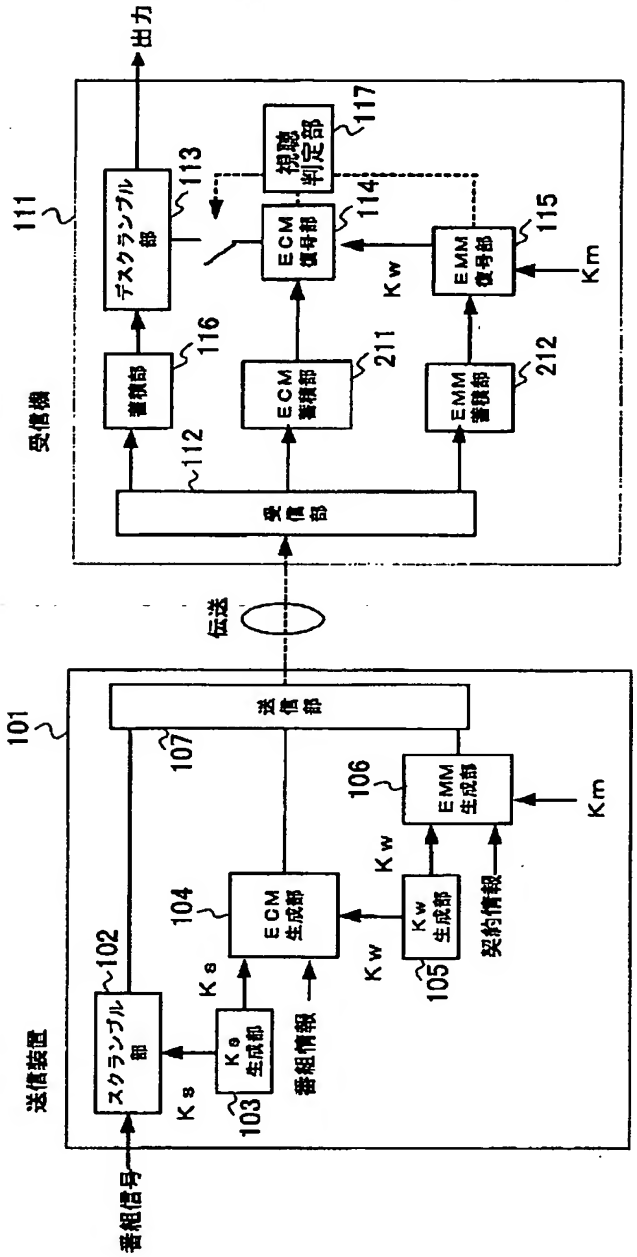
【図１】

従来の限定受信システムの第一の構成例



【図２】

従来の限定受信システムの第二の構成例



【図５】

本発明を使用した限定受信システムの一構成例